The U.S. Department of Energy

Training to Promote Local CI Awareness

October 2008

Promoting Local CI Awareness Training

Table of Contents

Training to Promote Local CI Awareness

Awareness Marketing:

CITD provides counterintelligence and terrorism awareness promotional items for all attendees to our classes. Products may include pen/highlighters, badge lanyards, calendars, etc.

Also available (on loan to your field or site CI office) is a large display panel for posters and other informational items that you may wish to post on-site for your local awareness promotion. The curved panel, covered in a medium blue background, has an attached solid title banner with CITD's logo. A local version can be printed at your site or prepared in advance through contact with CITD.

Tailored Awareness Products

We are your technical and professional resource for high-quality products to enhance and promote your local employee-awareness training program. Should you desire to meet local needs with a specialized or tailored presentation on any topic with a CI emphasis, contact the CITD Manager directly or e-mail us at CI@ntc.doe.gov.

Specialized or Tailored Briefing Topics

Are There Spies Among Us?

Whether you work in government or the private sector, the most dangerous threat to an organization is that of the person working inside the walls. The insider knows the security protocols, knows where the most critical information is kept, and knows the vulnerabilities of the people. Within a short period of time, the insider has the opportunity to loot an organization or recruit others to do it for him.

This 90-minute presentation includes a definition of the insider threat, why the insider is so successful, the volunteer and the recruit, the precursors to an act of espionage, psychological profile of the insider, and where to report individual concerns. Attendees also participate in a short case study and group exercises designed to reinforce the information presented.

Communicating with Scientists and Engineers: An Essential Element of Research Technology Protection Programs

The ability of U.S. counterintelligence (CI) to protect critical research and development assets is dependent on effectively communicating the threat posed by foreign entities to the science/engineering community which can be enhanced by understanding the culture of scientific collaboration and cooperatively working with the scientific community to reduce the risk of exploitation without impeding collaborative research. Scientists and engineers represent the intellectual capital upon which national and economic security depends. The United States has held a position of global leadership in science and engineering (S&E) which is attributed to both indigenous talent and contributions of scientist, engineers, and students from other countries.

Preservation of our global technological lead is highly dependent on continued open communication and foreign and domestic collaboration. While collaboration is essential for the culture and vitality of scientific research, it is not without the risk of providing information to our competitors and adversaries. Counterintelligence and security organizations by contrast usually seek to limit the exposure of Critical Program Information to compromise or disclosure. The U.S. research and development community remains a prime target for foreign exploitation, which can responsibly be mitigated through close collaboration with the CI community.

The challenge for the CI professional working in the environment of world-class science and research then is to understand the culture of collaboration and to communicate the value of critical risk management to the scientist/researcher who must, by nature and necessity, go "in harm's way" to conduct true research.

Ultimately, we must better understand the "culture of science," not change it.

The purpose of this discussion is to (1) examine how scientists think and work, (2) identify similarities between scientific research and law enforcement work, (3) discuss the very legitimate need for collaborative research, (4) describe the Scientist-to-Scientist Counterintelligence Awareness Program, and (5) provide insight on how the CI and scientific communities can cooperate to optimize scientific research and to protect sensitive information.

Conducting Research in a Threat Environment: Reducing the Risk of Exploitation

The Soviet Union's demise eased military and political tensions between the Superpowers, but did not bring a corresponding reduction in the level of espionage and other intelligence activities, which continue to target U.S. research and development (R&D) laboratories and threaten our national security. In recent congressional testimony, The National Counterintelligence Executive reported that "nearly 140 nations and some 35 known and suspected terrorists organizations currently target the United States for intelligence. Further, open source reporting indicates that Russia is fielding at least as many spies as were deployed by the old, much larger Soviet Union, and the number of clandestine intelligence operations conducted by the People's Republic of China is overwhelming.

Adversaries and allies alike are increasing their collection activities against the United States. Sensitive U.S. technologies (e.g., information technology, nuclear technology, weapons systems) remain prime targets for foreign acquisition, both lawful and illegal. Foreign companies, scientists, academics, and others see the acquisition of U.S. technology as a key to advancing their economic and military interests. Foreign entities seek to exploit visits to U.S. laboratories or contacts with laboratory personnel as a means of obtaining classified or other sensitive information.

The United States, and especially the U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) laboratories, represent the intellectual capital on which our national and economic security depends. The United States has held a position of global leadership in science and engineering which is attributed to both indigenous talent and contributions of scientist, engineers, and students from other countries. The nation's scientific and technical infrastructure is highly dependent on contributions of foreign-born scientists and engineers (S&E). Estimates from the 2000 Census indicate that 40-50% of the S&E doctorate-level workforce was foreign-born.

While collaborative research is essential for the culture and vitality of scientific research, it is not without the risk of providing information to our competitors and adversaries. These risks pose a challenge for counterintelligence. The role of counterintelligence is to work with the scientific community to reduce the risk of exploitation without impeding collaborative research.

The purpose of this briefing is to (1) increase awareness of the threat posed by foreign entities to DOE/NNSA assets, (2) discuss how the personal vulnerabilities of a national laboratory/university scientist and laboratory director were exploited to benefit a foreign entity, (3) describe the role of the DOE Office of Counterintelligence/NNSA Office of Defense Nuclear Counterintelligence in helping reduce the risk of exploitation, and (4) elicit your ideas on how to optimize scientific research while protecting national assets.

Deterring Threats to International Scientists and Researchers

Since its inception, the Department of Energy has benefited from the inclusion of international scientists and researchers. Many of the world's greatest achievements have come because of their efforts. These collaborations have led to the sharing of technological advances between the United States and the international community that have benefited everyone. Unfortunately, there are hostile elements in the world that would like to obtain that information for their own benefit. This is costly to our domestic and international researchers, who lose the recognition that

they have earned for their achievements, and to the Department of Energy, which has invested heavily in support of those achievements. The role of counterintelligence is to identify those hostile elements and stop them from gaining access to information for which they have no earned right.

During this 90-minute presentation, we list some of the targeted unclassified technologies. We also discuss the recruitment cycle and how it is used to compromise unsuspecting scientists and researchers. Finally, we discuss where you can go for help should you feel that someone is trying to target you and your research.

Economic Espionage: Threat to DOE/NNSA Assets

The lessening of tensions between the Superpowers at the end of the 20th Century enabled our adversaries to allocate a greater portion of their foreign intelligence services' resources to collecting sensitive U.S. technology and economic information, which poses a serious threat to national security. The United States, especially the Department of Energy (DOE) and National Nuclear Security Administration (NNSA) complex, is at the center of the world's research and development enterprise. Sensitive U.S. technologies—those that both underpin the U.S. economy and contribute to U.S. military prowess—remain prime targets for foreign acquisition, both lawful and illegal.

Foreign theft of sensitive technology has undercut the competitiveness of U.S. industry by allowing foreign firms to acquire, at little or no cost, technology that U.S. firms spent hundreds of millions of dollars developing. Open source reporting indicates that Russia is fielding at least as many spies as were deployed by the old, much larger Soviet Union, and the number of clandestine intelligence operations conducted by the People's Republic of China is overwhelming. Even some close U.S. allies actively seek to obtain classified and technical information from the United States through unauthorized means. In fiscal year 2004, the counterintelligence community tracked the efforts of foreign businessmen, scientists, academics, students, and government entities from almost 100 countries to acquire sensitive U.S. technologies. While the number of countries targeting U.S. technology is large, about 60% of the activity can be attributed to 10 countries, with China and Russia ranking near the top of the list. In a candid interview, Pierre Marion, former director of French intelligence, said

"We are military allies, but economic competitors. Therefore, industrial espionage, even among friends, is a normal action of an intelligence agency."

The purpose of this briefing is to (1) increase awareness of the threat posed by foreign entities to DOE/NNSA assets; (2) discuss how foreign governments, corporations, and individuals are exploiting DOE/NNSA assets (people, facilities, information) for their benefit; and (3) discuss how the DOE/NNSA Office of Counterintelligence can help you manage the risk.

Elicitation: The Exploitation of Conversation

Elicitation is a collection of techniques used in conversational situations to acquire information from someone (source) without being obvious. We all use elicitation day-to-day (e.g., sales people, parents, boyfriends/girlfriends, doctors, scientists/engineers). It is an accepted form of social discourse. In the espionage trade, however, it is used to covertly manipulate someone, to subtly extract information about you, your colleagues, or your work.

Elicitation appears to be normal social or professional conversation and can occur anywhere—in a restaurant, at a conference, during a visit to one's home, or any other business/social gathering. As an intelligence gathering technique, elicitation is appealing because it is non-threatening, easily disguised, and exploits several fundamental aspects of human nature.

The purpose of this briefing is to (1) discuss why elicitation is an effective method of obtaining information, (2) show elicitation in action, and (3) discuss countermeasures.

Espionage: Continuing Threat to U.S. National Security

Foreign individuals from both the private and public sectors in almost 100 countries attempted to acquire sensitive U.S. technologies in fiscal year 2004, which has resulted in the erosion of the U.S. military advantage and degraded the U.S. intelligence community's ability to counter espionage and terrorist threats. About 60% of the espionage activity can be attributed to 10 countries, with our old Cold War adversaries, China and Russia, ranking near the top of the list and long-standing allies (e.g., France, India, Israel) also being major espionage threats.

Open source reporting indicates that Russia is fielding at least as many spies as were deployed by the old, much larger Soviet Union. The information our competitors and adversaries seek is not simply political or military data but also science and technology, financial, and commercial information. These continuing threats pose a challenge for counterintelligence as the tension between open science and national security issues builds.

The purpose of this classified briefing (Secret) is to (1) identify foreign entities targeting U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) assets, (2) discuss the methods of operation, and (3) discuss how you and the DOE Office of Counterintelligence or NNSA Office of Defense Nuclear Counterintelligence can help reduce the risk of exploitation.

Food and Agricultural Security: Threats, Vulnerabilities, and Consequences

Agriculture and food systems are essential commodities in the United States and remain vulnerable to deliberate attacks which could have significant impacts on social, economic, and political stability. In 2002 (latest data available), food and agriculture industries contributed $1.29 trillion worth of value added to the economy, which accounted for over 12% of the U.S. gross domestic product and employed 17% of all U.S. workers. Further, the United States exported $53.3 billion of agricultural products (a $12.3 billon trade surplus) accounting for 8% of all U.S. goods exported.

Several governments, including the United States, developed anti-crop and anti-animal weapons for use during war situations. Some countries continue to support biological warfare programs in spite of international treaty prohibitions. Terrorist groups, both state-sponsored and others, are attempting to acquire and deploy these weapons. The United States' agricultural system is especially vulnerable to these attacks because of our modern crop and animal production practices and they are considered soft-targets. Aimed at the nation's food supply system, these attacks could have significant health, economic, psychological, and political consequences that are, perhaps, more devastating than attacks on the human population.

The magnitude of the potential economic impacts can be drawn from the dioxin-contaminated feed situation in Belgium during the spring/summer of 1999. The ensuing crisis brought Belgian

trade to a virtual standstill, costing the country billions of US dollars, and brought down the government.

The purpose of this presentation is to (1) discuss who may threaten our agricultural and food supply systems, (2) describe the system's vulnerability, (3) discuss the potential consequences resulting from an attack, (4) discuss the U.S. Department of Energy's interest, and (5) discuss how you can assist in protecting this critical infrastructure.

Foreign Visitors & Assignees: Potential Target for Hostile Intelligence Services

Each year, U.S. Department of Energy (DOE) and National Nuclear Security Administration (NNSA) sites host thousands of foreign visitors and assignees (FV&A) who not only contribute greatly to advancing the DOE/NNSA scientific enterprise but, also are targeted for exploitation by hostile intelligence services. International students and scholars have advanced U.S. science and engineering (S&E), as evidenced by numbers of patents, publications, Nobel prizes, and other quantitative measures.

Since 1990, almost half of the U.S. Nobel laureates in science fields were foreign-born. As a result of the increasing globalization of science we are, more than ever before, dependent on international collaboration. In general, all DOE/NNSA research, including its classified work, is built on unclassified science. This unclassified work is highly dependent on international interactions and on a workforce comprising large numbers of foreign-born scientists and engineers. For example, some major high-energy physics experiments are run by teams of physicist and engineers, half of whom are foreign.

The continued success of the DOE/NNSA laboratories depends on the ability to collaborate internationally and to recruit and retain scientists and engineers born outside the United States. For the year ending 31 August 2005, DOE/NNSA facilities received over 45,000 FV&A requests with almost 40% being for sensitive country foreign nationals. Foreign entities continue to unlawfully target or acquire critical U.S. technologies, trade secrets, and sensitive financial or proprietary economic information.

The amount of FV&A activity in the DOE/NNSA community provides ample opportunity for a HIS to exploit resident visitors and assignees or insert co-opted scientists into our programs.

The purpose of this briefing is to (1) identify countries currently targeting DOE/NNSA assets; (2) discuss their methods of operation; (3) describe defensive tactics for hosts, escorts, visitors and assignees; and (4) describe how the DOE Office of Counterintelligence or NNSA Office of Defense Nuclear Counterintelligence can help you reduce the risk of exploitation.

Information Technology: Essential Research Tool or Critical Vulnerability

The dramatic change in the way we collaborate, enabled by the global proliferation of information technology (IT), has spurred scientific innovation and economic growth but leaves us vulnerable to exploitation. Government, commercial, educational, and research organizations depend on IT to conduct day-to-day operations. Information technology provides access to colleagues, journals, reference rooms, and databases, and provides the computational power to help understand the fundamental processes governing the world in which we live.

Problems in physical science ranging from magnetohydrodynamics, to simulating energetic particles and plasma turbulence, and data analysis as well as other complex physical problems (climate change, computational fluid dynamics) present challenging computational problems requiring enormous amounts of computer time. Work in plasma physics has contributed significantly to progress in IT and scientific computing. Massively distributed parallel processing, grids (e.g., Fusion Grid), and clusters offer networked capabilities to help solve these problems. Our increasing dependency on these networked systems provides opportunities for malicious activity. Significant weaknesses in computer systems put critical operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

A spectrum of malicious actors can and do conduct attacks against IT.

The purpose of this briefing is to (1) identify threats to information technology, (2) discuss system vulnerabilities, (3) describe methods used to exploit systems and people, and (4) discuss how the U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) Office of Counterintelligence can help you reduce the risk.

Intellectual Property Competition: Exploitation, Theft, or Collaboration

The tradition of open exchange and collegial atmosphere, which is the cornerstone of our scientific method of discovery, has enabled others to acquire and exploit information, gaining competitive advantage, resulting in lost opportunities. Misappropriation of sensitive information continues to grow as a problem for U.S. government and businesses, costing billions dollars and compromising our national security.

All categories of critical technologies continue to be the subject of foreign interest for military and economic exploitation. The information they seek is not simply technological or military data but also financial and commercial information that will give their countries a competitive edge in the global economy.

The United States remains a prime target of foreign economic collection and industrial espionage. Economic collection against the United States, including the theft of trade secrets and competitive business information, is likely to intensify in the new millennium as the race to control scarce resources and global markets intensifies. Adversaries and allies alike increased their collection activities against the United States, while developing countries are recognized as new competitors, increasing the threat.

Open source reporting indicates that Russia is fielding at least as many spies as were deployed by the old, much larger Soviet Union.

The purpose of this seminar is to (1) increase your awareness of the threat to DOE/NNSA intellectual property posed by foreign entities, (2) characterize potential consequences of a loss event, (3) identify technologies of interest, and (4) discuss your role in helping protect intellectual property.

Loose Lips Lose Data

Foreign intelligence services often use what appears to be benign conversation as a method of obtaining information. A conversation can yield information that may fill a need unknown to the victim but is important to the elicitor. Only with knowledge of this method can we protect ourselves from unwittingly divulging sensitive information about ourselves and our work. The key to the success of this method is an individual's lack of awareness that he or she is being elicited.

This 90-minute presentation includes a definition of Elicitation, methods used by foreign intelligence services, individual vulnerabilities to this method, and where to report individual concerns. Attendees also participate in a short case study and group exercises designed to reinforce the information presented.

Management in a National Security Environment: Protecting DOE/NNSA Assets

The U.S. Department of Energy (DOE) and National Nuclear Security Administration (NNSA) scientific community represents the intellectual capital that our national and economic security depends. Further, the DOE/NNSA manages a large portfolio of collaborative relationships between laboratories and non-federal parties engaged in technology innovation and discovery to benefit society. Maintenance of our global technological lead is essential for maintaining our way of life and is highly dependent on open communication and foreign and domestic collaboration. DOE/NNSA laboratories provide critical assets in helping our nation secure a peaceful and free world through technology.

Adversaries and allies alike are increasing their collection activities against the United States. Foreign nations seek to exploit visits to the laboratory or contacts with laboratory personnel as a means of obtaining classified or other sensitive information. The information they seek is not simply technological or military data but also financial and commercial information. The national laboratories remain a prime target of foreign economic collection and industrial espionage as the race to control scarce resources and global markets intensifies. The DOE/NNSA counterintelligence community is looking to DOE/NNSA management to find ways that we can work within the "culture of science" to provide effective protection of DOE/NNSA assets and make a positive contribution to the integrity, reputation, and recognition of the DOE/NNSA scientific mission.

The purpose of this briefing is to increase your awareness of the role counterintelligence plays in DOE/NNSA strategic business planning and to engage DOE/NNSA managers in developing a counterintelligence strategy to detect, deter, and mitigate the threat to DOE/NNSA assets.

Mitigating the Foreign Threat to U.S. Scientists and Engineers: An Innovative Counterintelligence Awareness Program

Collaborative research not only is the basis for sustaining technological innovation, but also provides opportunities for our foreign adversaries and competitors to exploit these relationships causing damage to our programs and people. The role of counterintelligence is to work with the scientific community to reduce the risk of exploitation without impeding collaborative research. To meet this challenge the Counterintelligence Training Department (CITD) developed a Scientist-to-Scientist (S2S) counterintelligence awareness program to reach out and engage the

scientific and engineering community. The program draws on the background of a U.S. Department of Energy scientist, university researcher, and laboratory director with more than 30 years of laboratory and 10 years of intelligence and counterintelligence experience who provides unique insights into the problems of conducting open research in the high threat environment in which we now live.

Scientist-to-scientist counterintelligence briefings focus on site-specific issues, ensuring they are relevant and customized for a given audience (e.g., material scientists, plasma physicists). Topics are wide ranging and include open science and national security, foreign travel threats, information technology, foreign visits and assignments, social engineering, insider threats, food and agriculture security, weapons of mass destruction, technology transfer/partnerships, intellectual property, economic espionage, subcontracting, terrorism, and hostile intelligence threats. The value of these 30-minute to 2-hour presentations is evident in the number of counterintelligence referrals received from attendees, identifying previously unreported incidents of concern.

The purpose of this briefing is to describe the S2S program and provide examples from selected briefing topics.

DOE Power Marketing Administrations: Potential Target for Terrorists and Foreign Intelligence Organizations

The federal government produces about 10 percent of the electricity consumed in the United States and sells it through the Tennessee Valley Authority (TVA) and the four U.S. Department of Energy (DOE) Power Marketing Administrations (PMA). Although it constitutes only a small part of the national market, the federal power supply is important in certain regions of the country (e.g., Pacific Northwest). Further, PMAs provide the critical infrastructure which reliably and efficiently transmits tens of thousands of megawatts of power annually throughout the United States.

The federal government has identified 11 sectors of the economy that it deems critical to national security and essential to the functioning of the U.S. economy, which includes electrical power generation and transmission. This critical infrastructure is vulnerable to cyber-based attacks and more traditional attacks on physical structures. PMA facilities and infrastructure may be considered a soft target for physical attack, while the mission-critical Supervisory Control and Data Acquisition/Automatic Generation Control computer system would be of interest for cyber attack. The U.S. intelligence community considers energy technologies to be an essential element of information for many foreign intelligence organizations.

The purpose of this seminar is to (1) increase your awareness of the threat to PMA assets posed by foreign entities, (2) provide information to help you manage the risk of exploitation, and (3) discuss the role of DOE Office of Counterintelligence in helping you protect critical assets.

Recruiting the Spy

The recruitment of the insider to steal critical information is a process that takes time and skill to execute. Without the knowledge that recruitment is in progress, a person can unwittingly give away significant information before the recruiter asks for help. Employees must be armed with a basic awareness of the recruitment cycle and how their vulnerabilities may be used against them.

This 90-minute presentation includes a description of the recruitment cycle, key points in the cycle where recruitment can be deterred, human vulnerabilities to this method, and where to report individual concerns.

DOE/NNSA Research and Development Contracts: Exploitation by Foreign Entities

The U.S. Department of Energy (DOE), including the National Nuclear Security Administration (NNSA), executes much of its mission through contracts with the private sector, which provides opportunities for foreign entities to acquire and exploit DOE assets (i.e., information, people, and facilities).

The DOE spends more on contracting than any other civilian agency in the federal government. In fiscal year 2004, the DOE spent over $22 billion on contracts with over $3 billion going to small businesses, fostering the innovation necessary to meet the nation's scientific and technological challenges. Due to the nature of the work, contractors often require access to sensitive financial or proprietary information, intellectual property, and classified information. Attempts by foreign agents to obtain sensitive information from contractors have increased over the last several years, and government officials expect this trend to continue.

Foreign businesspersons, scientists, academics, government officials, and hostile intelligence services continue aggressive targeting of U.S. technologies. Information losses could undermine U.S. military superiority, impede the ability of the United States to compete in the world marketplace, and/or have an adverse effect on the U.S. economy, eventually weakening national security.

The large volume of contracts under review at any time makes it difficult to vet all contractors.

The purpose of this presentation is to (1) increase awareness of the threat posed by foreign entities to DOE/NNSA assets, (2) discuss how U.S.- based foreign corporations are exploiting DOE/NNSA research and development contracts, (3) provide you with some tools to help identify

Risky Business: Threats to the Foreign Traveler

Each year, thousands of U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) employees and contractors travel all over the world (including DOE sensitive countries) to attend meetings and conferences, conduct research, or enjoy a holiday, all of which provide hostile intelligence services (HIS) the opportunity to conduct espionage activities against these travelers.

Since the early 1990s, DOE/NNSA laboratories have, quite properly, become more open and engaged in cooperative research with colleagues from other countries. DOE encourages international collaboration in its unclassified energy and science programs and in nonproliferation areas. Many of these collaborations occur, by choice or out of necessity, in the foreign collaborator's home country. Traveling to a foreign country can be an extraordinarily productive and exciting experience, but is not without risk.

Foreign countries are becoming increasingly aggressive in exploiting U.S. experts traveling abroad. As a DOE/NNSA employee or contractor, you could become the target for espionage, theft, terrorism, or kidnapping anytime in any country. You yourself may even increase the

likelihood that a HIS will develop an interest in you by actions you take that draw their attention to you. Once a service has spotted you, they assess your vulnerabilities and use this information to develop a plan of exploitation. While traveling abroad, you are on the host country's home turf, where the local intelligence services have many resources available. The rules that govern their activities are much different from those with which we are familiar. They can, and do, monitor and control the environment in which you live and work.

The purpose of this briefing is to (1) identify the risk to DOE/NNSA travelers while abroad, (2) discuss HIS methods of operation, and (3) discuss how you and the DOE Office of Counterintelligence or NNSA Office of Defense Nuclear Counterintelligence can help reduce your risk.

Scientist-to-Scientist Counterintelligence Awareness Program: A Veritable Smorgasbord of Topics

The Scientist-to-Scientist (S2S) counterintelligence awareness program is designed to reach out and engage the scientific and engineering community. The program draws on the background of a U.S. Department of Energy scientist, university researcher, and laboratory director with more than 30 years of laboratory and 10 years of intelligence and counterintelligence experience who provides unique insights into the problems of conducting open research in the high threat environment in which we now live. Scientist-to-scientist counterintelligence briefings focus on site-specific issues and wide ranging topics, ensuring they are relevant and customized for a given audience. The value of these 30 minute to 2-hour presentations is evident in the number of counterintelligence referrals received from attendees, identifying previously unreported incidents of concern.

The purpose of this briefing is to provide examples of slides/graphics used to highlight critical issues covered in several S2S briefings and discuss the philosophy governing their design

Social Engineering: Exploiting American Culture for Foreign Benefit

Social engineering is a tactic that exploits human behavioral traits to obtain sensitive information, without the "target" knowing they are being manipulated, to degrade programs or benefit a foreign nation or competitor. The 'fall of communism" did not reduce the level or amount of espionage activity conducted against the United States. On the contrary, foreign intelligence activities against the United States have grown in diversity and complexity. Hostile intelligence services continue to pursue traditional targets (military/political) while increasing their collection activities against economic and advanced technology targets.

The human factor is our weakest link, especially in America where we have a false sense of security and are somewhat naïve about the nefarious nature of those who wish to harm us. Our cultural and behavioral attributes (e.g., trusting, polite, helpful, honest) enable the "social engineer" to dupe us into supplying sensitive information or allowing inappropriate access to facilities or cyber systems.

The purpose of this briefing is to (1) discuss the risk posed by foreign/criminal entities to U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) employees and contractors, (2) discuss how social engineering is used to exploit Americans, and (3) discuss how

the DOE Office of Counterintelligence or NNSA Office of Defense Nuclear Counterintelligence can help you reduce your risk.

Technology Transfer and Related Technology Partnerships: Collaborative Innovation or National Security Threat

The transfer of U.S. Department of Energy (DOE) and National Nuclear Security Administration (NNSA) technology outside the government not only is a great opportunity for economic development, but also provides opportunities for others to acquire and exploit information. The DOE/NNSA promotes technology transfer using a variety of partnering mechanisms. These technology partnerships enable both parties to meet common goals while leveraging limited resources and reducing technology development risk.

In fiscal year 2004, DOE/NNSA and its laboratories and facilities negotiated and executed 10,091 technology partnership-related transactions. Economic espionage—theft of our intellectual property—is on the rise as the race to control scarce resources and global markets intensifies. A nation's national security and power is no longer measured only by military might but increasingly in terms of economic strength. Today's adversaries cannot be identified only by looking at some Cold War criteria. From an economic view, we do not have adversaries, in the traditional sense; we have competitors for market share. A recent Federal Bureau of Investigation survey of private sector research and development companies identified some of our Cold War adversaries (e.g., Russia, China) and longstanding allies (France, India, Israel) as being major economic espionage threats.

The purpose of this seminar is to (1) increase your awareness of the threat to DOE/NNSA critical technologies posed by foreign entities, (2) discuss how foreign entities are exploiting DOE/NNSA technical partnership opportunities for their benefit, and (3) discuss how the DOE/NNSA Office of Counterintelligence can help you manage the risk.

Terrorist Threats to DOE/NNSA Assets: Reducing the Risk

The risk of a terrorist attack against U.S. interests at home and abroad is real (probability >0) but can be reduced through a collaborative effort between the U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) counterintelligence element and DOE/NNSA employees and contractors. Terrorism is by no means a form of warfare unique to the present era; it is as old as the human race. Flavius Josephus, a priest, soldier, and scholar in the 1st Century CE, wrote of the Sicarii robbers in Jerusalem who would mingle among the multitude and kill those who were their enemies. He observed "the fear men were in of being so served was more afflicting than the calamity itself."

What distinguishes the present era from previous periods in history is the coincidence between vastly greater means available to terrorists and the increasing number of targets. The nature of terrorism has changed dramatically since the last of the 20th Century. While the number of terrorist attacks has been decreasing, the lethality of those attacks has been increasing. Further, terrorists have become more indiscriminate in their targeting and less constrained in the methods employed. Events in the United States over the past decade raise our level of concern about terrorists and their actions while frustrating us because of the difficulty in detecting and neutralizing terrorists before an attack. Further, it is difficult for the general population to assess personal risk because of conflicting media reports about the likelihood of an attack and its resulting consequences.

The purpose of this briefing is to (1) describe the nature of terrorism, (2) identify methods of operation, (3) identify indicators of terrorist activity, (4) discuss defensive tactics, and (5) discuss how you can assist the DOE Office of Counterintelligence and the NNSA Office of Defense Nuclear Counterintelligence in helping to protect DOE/NNSA assets.

The Invisible World of Foreign Intelligence

Every country in the world, those we consider friend as well as those we consider foe, has a responsibility to improve its position in the global economy. Working together with scientists from across the globe, we have helped many nations to improve life for their citizens using innovative technological solutions that they could not have developed alone. This nation has no problem sharing information with its neighbors; it does have a problem with those who use espionage as method to steal information to which they are not entitled. This includes not only weapons data, but also information that can be used to improve the economic position of one nation at the expense of another.

This 90-minute presentation includes a definition of the Foreign Intelligence Threat, methods used by foreign intelligence services, individual vulnerabilities, and where to report individual concerns. It also briefly discusses how computers have become a collection tool for foreign intelligence. Finally, attendees participate in a short case study and group exercises designed to reinforce the information presented.

Capturing Jonathan Pollard

Two decades have passed, and events have unfolded. It is now time for the inside and never-before-told facts of this espionage investigation to be revealed and shared with counterintelligence and security professionals. No other spy in the history of the United States has brought so much political controversy, media hype, and straining of relations between two allies than that of Jonathan Jay Pollard.

This 50-minute session will briefly touch on how the Navy had the opportunity to fire Pollard, and decided against it, long before Pollard became involved with Israel. Also included are how he was tasked by his Israeli handlers, uncovered and caught with his witting wife Anne, the interrogation, the volume of highly classified information he stole, and the political aftermath of this spy case, which continues to this day.

Trusted Insiders: The Threat from Within

Threats to U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) assets do not depend solely on the presence of a ruthless foreign adversary but may reside in the trusted insider who, through some combination of character weaknesses and situational stresses, decides to betray the laboratory. The threat from within may exceed that from external sources. Research shows that, by far, most of the Americans arrested for spying in the last 20 years have been volunteers or insiders.

The insider is different from the outsider because the former is granted certain access, authorities, and trust. Further, insiders have a superior knowledge of asset value, security protocols, and personnel. The consequences may be significant and can include a compromise of national security, damage to reputation, loss of business, and criminal or civil proceedings. Insider betrayal is not a new phenomenon identified when Federal Bureau of Investigation (FBI)

Special Agent Robert Phillip Hanssen admitted passing highly classified information to the Soviet Union/Russian Federation. Rather, it has been present throughout recorded history, from Sun Tzu who described inside agents as "enemy officials whom we employ" (~400 BCE) to inside betrayers like Brutus (44 BCE), Judas (~33 CE), and former Los Alamos National Laboratory scientist, Dr. Peter Hoong Yee Lee (1997 CE).

The purpose of this briefing is to (1) discuss the risk posed by insiders to DOE/NNSA assets, (2) identify the sources of insider problems, (3) describe at-risk behaviors for insider threats, and (4) discuss how the DOE Office of Counterintelligence or NNSA Office of Defense Nuclear Counterintelligence can help you reduce the risk.

Weapons of Mass Destruction: Countering the Threat

The risk of a terrorist attack involving weapons of mass destruction (WMD) against U.S. interests overseas and at home is real (probability > 0) but can be reduced through a collaborative effort between the U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) counterintelligence element and DOE/NNSA employees and contractors. Events in the United States over the past decade raise our level of concern about terrorists and their actions while frustrating us because of the difficulty in detecting and neutralizing terrorists before an attack. Further, it is difficult for the general population to assess personal risk because of conflicting media reports about the likelihood of a WMD attack and its resulting consequences.

The purpose of this presentation is to (1) describe various WMD categories, (2) provide insight into the relative probability of an attack, (3) add perspective to media estimates of potential consequences, and (4) discuss how you can assist the DOE Office of Counterintelligence and the NNSA Office of Defense Nuclear Counterintelligence in helping to protect DOE/NNSA assets.

Limited Graphics Support

- PowerPoint presentations
- Poster design and production
- Brochures design and production

(Please bear in mind that graphic support takes time, so advanced planning is a must.)